Applied Abstract Algebra. Lecture 1.

The purpose of the course is to introduce the concepts and theorems of Abstract Algebra that underlie modern communication algorithms.

This is a mathematical course. That's why I'll try to be precise and to provide rigorous proofs.

We will need all the basic concepts of Abstract Algebra: groups, rings, fields, vector spaces.

If you have already taken a course in Abstract Algebra then you will have a chance to review it again together with some

applications.

GROUPS.

Let X be a set, $n \geq 1$. The Cartesian power $X^n = \underbrace{X \times X \times \cdots \times X}_{n}$ is a set of tuples

$X^n = \{ (x_1, \ldots, x_n) \mid x_i \in X \}$.

An n-ary operation is a mapping $X^n \to X$.

Of particular interest are 2-ary (binary) operations $X^2 \xrightarrow{\varphi} X$. To every pair of elements $x, y \in X$ we assign their "product" (or "sum") $\varphi(x,y) \in X$.

Examples. 1) $X = \mathbb{R}$ real numbers, $\varphi(x,y) = x+y$

2) — " — , $\varphi(x,y) = x \cdot y$

3) — " — , $\varphi(x,y) = x^2 + y$

Sometimes we will denote $\varphi(x,y) = xy$, juxtaposition (not to confuse with multiplication of numbers).

Let G be a set with a binary operation

$G^2 \to G$, $(x,y) \to xy$.

Definition. We say that the binary operation $(x,y) \to xy$ is associative if $\forall x,y,z \in G$

$(xy)z = x(yz)$.

Examples 1), 2) above are associative. The example 3) is not.

Definition. A set G with a binary operation $(x,y) \to xy$ is called a group if

1) the operation $(x,y) \to xy$ is associative;

2) there exists an element $e \in G$ such that for an arbitrary element $x \in G$ we have $ex = xe = x$. Such an element is called an identity;

3) for an arbitrary element $x \in G$ there exists an element $y \in G$ and an identity $e \in G$ such that $xy = yx = e$. Such an element y is called an inverse of x.

First Theorem. 1) A group contains only one ~~inverse~~ identity;

2) every element has only one inverse.

Proof. 1) Let e, f be both identities. Then $ef = f$ because e is an identity.

On the other hand $ef = e$ because f is an identity. Hence $e = f$.

2) Let y, z be both inverses of an element $x \in G$

$$yx = xy = e,$$

$$zx = xz = e.$$

Then $(yx)z = e \cdot z = z$; $y(xz) = y \cdot e = y$.

But $(yx)z = y(xz)$ because of associativity.

Hence $y = z$. ↓

Examples of Groups.

1) $G = \mathbb{Z}$ or $\mathbb{Q}$ or $\mathbb{C}$ with addition;

2) $G = \mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$ or $\mathbb{R}^*$ or $\mathbb{C}^*$ with multiplication.

3) $GL(n, \mathbb{R}) = \{$ invertible $n \times n$ matrices over $\mathbb{R}$, multiplication $\}$

More Examples: reduction mod n.

Let $n \geq 2$ be a positive integer. Every integer a can be divided by n with a reminder,

$$a = qn + r, \quad 0 \leq r \leq n-1.$$

Let us define addition in the set of reminders $\mathbb{Z}(n) = \{0, 1, 2, \ldots, n-1\}$.

Let $0 \leq r_1, r_2 \leq n-1$.

If $r_1 + r_2 \leq n-1$ then $r_1 + r_2$ is a reminder.

If $r_1 + r_2 \geq n$ then this is not a reminder. We divide $r_1 + r_2$ by n

$$r_1 + r_2 = qn + r$$

and declare the sum of r_1 and r_2 to be r.

Let $n = 6$. Then $3 + 4 = 1$.

Identity element: 0. what is the inverse of 4? The inverse is 2. Indeed, $4 + 2 = 0$.

$\mathbb{Z}(n) = \{0, 1, 2, \ldots, n-1\}$ is a group with respect to thus defined addition.

Let $p \geq 2$ be a prime number.

Let $\mathbb{Z}(p)^* = \mathbb{Z}(p) \setminus \{0\} = \{1, 2, \dots, p-1\}$

be the set of nonzero remainders mod p.

Multiplication: as above.

If $i, j \in \mathbb{Z}(p)^*$ and $ij \geq p$ then

$ij = qp + r$, r is the remainder,

r is declared the product of ij.

Proposition. $\mathbb{Z}(p)^*$ is a group with respect to thus defined multiplication.

Proof. First we notice that $ij \in \mathbb{Z}(p^*)$ then $r \in \mathbb{Z}(p^*)$, i.e. $r \neq 0$. Indeed,

$r = 0 \iff ij$ is divisible by p.

If a product of two integers is divisible by a prime number p then at least one of these integers is divisible by p. The numbers i and j are not divisible by $p \Rightarrow z$ is not divisible by p.

Consider $(\mathbb{Z}(p)^*, \cdot)$.

The multiplication is associative; there exists an identity element 1. We need to check that every element of $\mathbb{Z}(p)^*$ has an inverse.

Let $a \in \mathbb{Z}(p)^*$, $1 \leq a \leq p-1$. All products

$a \cdot 1, a \cdot 2, \ldots, a \cdot (p-1)$

are distinct. Indeed, let

$$a \cdot i = a \cdot j, \quad 1 \leq i < j \leq p-1.$$

Then $a(j-i) = 0 \mod p$.

Both numbers a and $j-i$ lie between 1 and $p-1$, hence are not divisible by p. This implies that $a(j-i)$ is not divisible by p. Hence

$$\{a \cdot 1, a \cdot 2, \ldots, a \cdot (p-1)\} = \{1, 2, \ldots, p-1\}.$$

Hence there exists $1 \leq b \leq p-1$ such that $a \cdot b = 1 \mod p$, $b = a^{-1}$. ↓

$$|\mathbb{Z}(p)^*| = p-1.$$

Isomorphisms.

Let G_1, G_2 be groups. A mapping

$$\varphi : G_1 \to G_2$$

is called an isomorphism if

(1) φ is a bijection,

(2) $\forall a, b \in G_1 \quad \varphi(ab) = \varphi(a)\varphi(b)$

We say: φ preserves multiplication.

Example. Let $G_1 = (\mathbb{R}, +)$, $G_2 = (\mathbb{R}_{>0}, \cdot)$.

Here $\mathbb{R}_{>0} = \{$all positive real numbers$\}$,

$$\varphi(a) = e^a$$

$$e^{a+b} = e^a \cdot e^b$$

An isomorphism $\varphi : G \to G$ is called an ~~isom~~ automorphism.

Examples. 1) The mapping $\varphi(n) = -n$ is an automorphism of $(\mathbb{Z}, +)$.

2) The conjugation mapping $\varphi(z) = \overline{z}$ is an isomorphism of the group $(\mathbb{C}, +)$.

3) The mapping $A \to (A^t)^{-1}$ is an automorphism of $GL(n, \mathbb{R})$

1), 2) are obvious. The 3d example is an exercise.

Exercise. Let $\varphi : G_1 \to G_2$ be an isomorphism. Let e_1, e_2 be identity elements of the groups G_1, G_2 respectively. Then

$\varphi(e_1) = e_2$ and $\forall g \in G_1 \ \varphi(g^{-1}) = \varphi(g)^{-1}$.

Exercise. If $\varphi : G_1 \to G_2$ is an isomorphism then the inverse map $\varphi^{-1} : G_2 \to G_1$ is also an isomorphism.

A property (P) is called abstract if it is invariant with respect to isomorphisms, that is, if $G_1 \cong G_2$ and G_1 has (P) then G_2 also has (P). We study only abstract properties. In other words we don't distinguish between isomorphic groups.

A group = (a set, an operation).

Which is more important?

Answer: operation.

Def. A group G is called **cyclic** if there exists an element $a \in G$ such that

$$G = \{a^i,\ i \in \mathbb{Z}\}.$$

Here $a^{-5} = (a^{-1})^5 = (a^5)^{-1}$.

Examples. $(\mathbb{Z}, +)$ and $(\mathbb{Z}(n), +)$ are cyclic groups.

Def. A group G is called **abelian** if

$\forall a, b \in G \quad ab = ba$.

Groups $(\mathbb{C}, +)$ and $(\mathbb{C} \setminus \{0\}, \cdot)$ are abelian.

The group $GL(2,\mathbb{R})$ is not abelian.

Let $a = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, $b = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$. Then

$$ab = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix};$$

$$ba = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}.$$

Being a finite group, being a cyclic group, being an abelian group are abstract properties.